

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

This invention relates to the processor which starts the field of a processing system, especially is used for a code system.

[0002]

[Background of the Invention]

Use of the code for encoding an electronic contents ingredient is increasing. In the amusement field, a digital audio and video record are enciphered in order to protect the subject matter concerned from an unjust copy. In the communication link field, a document is used, in order that it may be enciphered in order to prevent **** without authorization, and the enciphered certification may verify authentication of a document.

[0003]

Much specification for enciphering a security item like the ticket relevant to access to a copyright contents ingredient or this copyright contents ingredient whenever a subject matter is transmitted to other things from a certain equipment is adopted or proposed. For example, when CD recorder creates CD including the copy of the subject matter from which the duplicate was protected "based", this record is protected in code so that only the CD player "based" can reproduce this subject matter. The equipment "based" is equipment which performs adopted specification. the contents ingredient from which the original duplicate was protected — "a 1-time copy (copy-once)" — CD recorder based when it had the limit of a duplicate — this original copy — "it being unable to copy (copy-never)" — a display is attached in code. Based CD recorder understands this "a copy is impossible" display, and the copy of this copy does not create. When copied by the recorder by which this subject matter is not based, the based recorder or regenerative apparatus does not perform this copied record or playback of a subject matter excluding a code item with this appropriate copy.

[0004]

Specification is adopted in order to encipher an E-mail document and a contents ingredient like an attachment transmitted, to sign and to attest. A code security item which a contents ingredient is enciphered or identifies the transmitting origin of this contents ingredient into a contents ingredient is attached. "It joins together" into this ingredient in the form where it identifies whether this security item was changed after this contents ingredient was first transmitted for decode of this security item. [attach or]

[0005]

Installation of the encryption equipment to encryption, the above-mentioned example of the increment in use of decode, and an electronic instrument especially with the various increment in a code-signature and use of an access ticket in a verification list or decode equipment is needed. All the audios, video records, or regenerative apparatus that were based must include a means to process or exchange a key or other security items, including both equipments of a quiescence mold and a pocket mold, and must usually contain code-signature equipment, verification equipment, or both. It is expected that all E-mail transmission or receiving sets will contain signature equipment, verification equipment, or both also including multiplex functional equipments, such as a cellular phone. Thus, the request to a processor which makes easy code-signature in various systems, verification, and processing of a key exists.

[0006]

Although a special order design circuit may be the cheapest example of the equipment which carries out encryption or decode processing of a digital signature, verification, and other authentication working-level months, development of cryptography invites the danger that the operation-ized algorithm will become old. Although a general-purpose programmable processor makes it possible to change the operation-ized algorithm as encoding technology changes, and introduced into all the equipments that require encryption capacity, it is not necessarily economically possible. A low-price general-purpose processor cannot attain the target engine performance expected to authentication processing of real time, but, probably, is needed as an auxiliary device or a high speed processor is also by the increment in a price. Even if the target of a price is fulfilled by a low-price processor and the auxiliary device, physical constraint of systems to hold, such as a cellular phone, may eliminate use of these auxiliary devices.

[0007]

[Description of the Invention]

One purpose of this invention is to offer the programmable processing system which easy-izes code-authentication.

Moreover, other purposes of this invention are to offer the code processing system optimized to common encryption and a decode utility feature. Moreover, the purpose of further others of this invention is to offer a low price code processing system.

[0008]

These purposes and other purposes are attained by offering the processor architecture and the instruction set which fitted cipher processing good especially. In order to minimize the complexity of a design and to minimize the complexity of interconnect in equipment, various techniques are used, and this reduces the surface area needed and a related price. moreover, the activity whose various techniques program a processor for cipher processing — easy — izing — and ** — it is used in order to optimize the effectiveness of the instruction expected to be used in common by programming of processing [like]. In the example of a desirable low price, the random access memory (RAM) of a single port is used for storage of an operand, and only few data buses and resists are used for a data path, but an instruction set is optimized to the parallel processing in an instruction. Since cipher processing was characterized by the operation to a data item with wide width of face, emphasis was put especially on efficient processing of two or more word operation also including use of a constant with the same width of face as instruction word. The simplified arithmetic operation unit which supports efficiently the function typically needed for cipher processing by the minimum overhead was prepared. In the desirable example, the instruction set of a microcode map mold was adopted so that two or more parallel processing which can be set to each instruction cycle might be easy-ized and direct processing control might be obtained by the minimum overhead.

[0009]

[Best Mode of Carrying Out the Invention]

Hereafter, this invention is explained to a detail with reference to an accompanying drawing in instantiation. In addition, it lets a complete diagram pass and the same sign shows the description or the function to be this appearance or to correspond. Moreover, through the following explanation, the sign between 100 and 199 shows the item in drawing 1 , the sign between 200 and 299 shows the item in drawing 2 , the sign between 300 and 399 shows the item in drawing 3 , and the sign between 400 and 499 shows the item in drawing 4 .

[0010]

It is based on recognition that this invention is a thing in connection with simple arithmetic operation processing relatively although cipher processing, such as the message exchange of a digital signature and verification, public presentation / private key, is concerned with a typically big data variable. The usual algorithm for authentication systems is a digital signature algorithm (DSA). Other usual algorithms proposed as a digital signature and specification for verification (ANSI X9.62) are elliptic curve digital signature algorithms (ECDSA). This algorithm built into the digital transmission contents protection system (DTCP) was adopted as what is introduced into a digital audio and a video product equipped with IEEE-1394 connection. Above DCDSA is especially suitable for the low-price example good. Use of an elliptic curve is because it is a thing in connection with addition, subtraction, multiplication, and the simple mathematics operation of reversal.

[0011]

The dimension of the data variable used for a digital signature and verification is large, and is 160 or 320-bit width of face typically. In order to divide this data item into 5 or 10 words at homogeneity, in a desirable example, the data word dimension of 32-bit width of face is used. The data word dimension chosen is compromise on a design. That is, a big WORD dimension needs additional wiring and additional routing, and a small WORD dimension needs an additional WORD operation for per data item. It recognizes applying the overhead of remarkable wiring and routing to broad data word, and the data flow and the control structure by this invention are sharply restricted to it compared with the conventional processing system.

[0012]

In a desirable example, in order to minimize the complexity of a circuit, and routing, single RAM for variables is desirable in an instruction and single ROM for constants, and a list. A data constant is the same desirable dimension as data word, and since the same desirable ROM as an instruction memorizes, the instruction word dimension in a desirable example is made equal to a data word dimension.

[0013]

The above-mentioned simple mathematics operation to a data item suggests the instruction of the minimum number needed, and an instruction word dimension equal to the data word dimension suitable for a broad data item enables the instruction with which a large number differ. It recognizes that the rate of processing is important, and to each instruction, according to this invention, available 32 bits are constituted so that two or more parallel processing may be made possible within each instruction.

[0014]

Drawing 1 shows the instantiation-block diagram of the data flow architecture 100 of the processing system by this invention. This processing system is optimized so that the complexity of routing may serve as min compared with the conventional 32-bit processing system, so that the simplicity of this block diagram may show. It is important that it is cautious of the arithmetic operation unit (AU) 110 only not having with an adder 112 and two pre-treatment equipments 114 and 116. The coordination of an operation which easy-izes parallel processing is obtained by this simplicity. Furthermore, I hear that memory 120 notices important one about it being single-port RAM equipped only with the minimum output fan-out, and it has it. This minimum fan-out enables minimization of a data leading-about path at the same time it offers the coordination of the operation which makes parallel processing easy. Similarly, registers 130 and 140 consist of a single input from the output 111 of AU110, and a limited output.

For example, the contents of the address register 130 are supplied only in order to address RAM120, and by the design of the conventional processor, typically, as ordinarily, they cannot be supplied as an input to AU110 or other processors. By itself, a register 140 does not supply an output, but it is used in order to supply the condition bit for controlling a repeat operation like multiplication so that it may state below. The use to which these registers 130 and 140 were restricted minimizes routing of the interconnect needed for each register, and makes it possible to dimension-size registers 130 and 140 the optimal to the function offered. For example, an address register 130 has only the need of being only the width of face which is enough to cover the address range of memory 120, and, as for the scan register 140, has only the need of being only the width of face which is enough to hold the control flag of relation.

[0015]

The effectiveness and effectiveness of architecture 100 are illustrated the optimal about drawing 2 , and this drawing shows two instantiation instruction formats 201 and 202 by this invention. The instruction formats 201 and 202 have many common instruction fields so that it may see.

* NOTICES *

JPO and NCIP1 are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the processing system which has the processor constituted so that program instruction contained in memory might be executed. Said processor The program counter constituted so that degree the instruction address might be included, The stack constituted so that at least one return address corresponding to activation of subroutine call instruction might be included, It **** and said program instruction is said processor. When related branch condition is in the 1st condition A branch address is made to supply to said program counter as said degree instruction address. When said related branch condition is in the 2nd condition The processing system characterized by including the branching-Els-return instruction [like] which makes said at least one return address supply to said program counter as said degree instruction address.

[Claim 2] It is the processing system which has the processor constituted so that program instruction relevant to the data item which occupies two or more words in memory might be executed. It is the processing system which said processor has a status register which contains a status flag, and is characterized by said status flag containing at least one flag depending on two or more WORD to which the selected data item corresponds.

[Claim 3] In a processing system according to claim 2 said at least one flag The data zero flag which shows that each WORD of two or more WORD which forms said selected data item includes a zero value, each two or more words WORD which forms said selected data item A zero value is included except for the lowest WORD of two or more of said WORD which forms the present data item. and data 1 flag which shows that this lowest WORD includes the value of 1 — and — the most significant of two or more WORD which forms said selected data item — un— the data highest flag and ** which identify 0 words — processing system characterized by including at least one.

[Claim 4] The processor constituted so that the present instruction from an instruction register might be executed, The operand register constituted so that the operand processed by this processor might be supplied according to said present instruction, It is the processing system which ****. Said present instruction contains the flag "which a constant follows". Said processor when a flag [the above "a constant follows" of said present instruction] includes the 1st value Consecutive WORD is loaded to said operand register. It is the processing system which loads consecutive WORD to said instruction register in the following processor cycle when a flag [the above "a constant follows" of said present instruction] includes the 2nd value and which is characterized by being constituted like.

[Claim 5] Processor constituted so that program instruction might be executed Memory in which it is the memory constituted so that an operand might be included, and each operand has the operand address [/ in the memory concerned],

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2003-517671

(P2003-517671A)

(43) 公表日 平成15年5月27日 (2003.5.27)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 9/42	3 3 0	G 0 6 F 9/42	3 3 0 A 5 B 0 1 3
	3 1 0	9/30	3 1 0 B 5 B 0 3 3
	3 5 0		3 5 0 A 5 J 1 0 4
	3 7 0	9/38	3 7 0 X
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 Z
審査請求 未請求 予備審査請求 未請求 (全 34 頁)			

(21) 出願番号 特願2001-545927(P2001-545927)
 (86) (22) 出願日 平成12年12月7日 (2000.12.7)
 (85) 翻訳文提出日 平成13年8月16日 (2001.8.16)
 (86) 国際出願番号 PCT/EP00/12441
 (87) 国際公開番号 WO01/044900
 (87) 国際公開日 平成13年6月21日 (2001.6.21)
 (31) 優先権主張番号 09/466, 392
 (32) 優先日 平成11年12月17日 (1999.12.17)
 (33) 優先権主張国 米国 (US)
 (81) 指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, I T, LU, MC, NL, PT, SE, TR), J P, K R

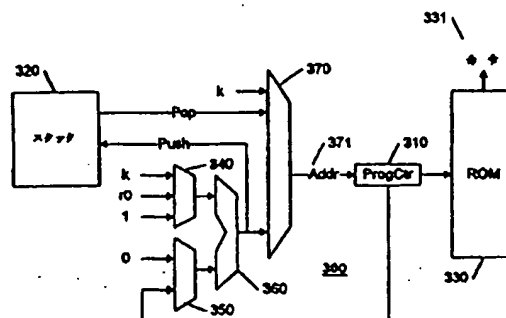
(71) 出願人 コーニンクレッカ フィリップス エレクトロニクス エヌ ヴィ
 Koninklijke Philips Electronics N. V.
 オランダ国 5621 ペーアー アインドーフェン フルーネヴァウツウェグ 1
 Groenewoudseweg 1,
 5621 BA Eindhoven, The Netherlands
 (72) 発明者 フレミング ジョージ エス
 オランダ国 5656 アーアー アインドーフェン プロフ ホルストラーン 6
 (74) 代理人 弁理士 神 経 進 (外1名)

最終頁に続く

(54) 【発明の名称】 単純なアルゴリズムの暗号エンジン

(57) 【要約】

暗号処理に特に良く適したプロセッサアーキテクチャ及び命令セットが提供される。設計の複雑さを最小化し且つ当該装置内の相互接続の複雑さを最小化するために種々の技術が採用され、これにより所要の表面面積及び関連するコストを減少させる。また、暗号処理用に当該プロセッサをプログラミングする作業を容易化し、斯様な処理のプログラミングに通常使用されると予想される命令の効率を最適化するために、種々の技術が使用される。好ましい低価格実施例においては、オランダの記憶のために単一ポートランダムアクセスメモリ (RAM) が使用され、データ経路には少ないデータバス及びレジスタが使用され、命令セットは命令内での並列処理のために最適化されている。暗号処理は幅の広いデータ項目に対する演算を特徴とするので、命令ワードと同一の幅を持つ定数の使用を含め、複数ワード演算の効率的な処理に重点が置かれている。暗号処理に典型的に必要なとされる機能を最小のオーバーヘッドで効率的にサポートするような単純なアーキテクチャユニットが提供される。各命令サイクルにおいての複数の並列処理を容易化



【特許請求の範囲】

【請求項1】 メモリに含まれるプログラム命令を実行するよう構成されたプロセッサを有する処理システムであって、前記プロセッサは、
次命令アドレスを含むように構成されたプログラムカウンタと、
サブルーチンコール命令の実行に対応する少なくとも1つのリターンアドレスを含むように構成されたスタックと、
を有し、前記プログラム命令が、前記プロセッサに、
関連する分岐条件が第1状態の場合には、前記プログラムカウンタに分岐アドレスを前記次命令アドレスとして投入させ、

前記関連する分岐条件が第2状態の場合には、前記プログラムカウンタに前記少なくとも1つのリターンアドレスを前記次命令アドレスとして投入させる、
ような分岐-エルス-リターン命令を含んでいることを特徴とする処理システム。

【請求項2】 メモリ内の複数ワードを占有するデータ項目に関連するプログラム命令を実行するよう構成されたプロセッサを有する処理システムであって

前記プロセッサは状態フラグを含むような状態レジスタを有し、前記状態フラグは、選択されたデータ項目の対応する複数のワードに依存する少なくとも1つのフラグを含んでいることを特徴とする処理システム。

【請求項3】 請求項2に記載の処理システムにおいて、前記少なくとも1つのフラグが、

前記選択されたデータ項目を形成する複数のワードの各ワードが零値を含むことを示すデータ零フラグ、

前記選択されたデータ項目を形成する複数ワードの各ワードが、現データ項目を形成する前記複数のワードの最下位ワードを除き零値を含み、且つ、該最下位ワードが1の値を含むことを示すデータ1フラグ、及び

前記選択されたデータ項目を形成する複数のワードの最上位の非零ワードを識別するデータ最高フラグ、
のうちの少なくとも1つを含むことを特徴とする処理システム。

【請求項4】 命令レジスタからの現命令を実行するよう構成されたプロ

セッサと、

該プロセッサにより処理するオペランドを前記現命令に応じて供給するように
構成されたオペランドレジスタと、

を有する処理システムであって、

前記現命令は“定数が後続する”フラグを含み、

前記プロセッサは、

前記現命令の前記“定数が後続する”フラグが第1値を含む場合は、後続のワ
ードを前記オペランドレジスタにロードし、

前記現命令の前記“定数が後続する”フラグが第2値を含む場合は、後続のワ
ードを次のプロセッササイクルにおいて前記命令レジスタにロードする、

ように構成されていることを特徴とする処理システム。

【請求項5】 プログラム命令を実行するように構成されたプロセッサと、

オペランドを含むように構成されたメモリであって、各オペランドが当該メモ
リ内に対応するオペランドアドレスを有するようなメモリと、

オペランドアドレスを含むように構成された少なくとも1つのアドレスレジス
タと、

を有する処理システムであって、

前記少なくとも1つのアドレスレジスタの各々が、

前記プロセッサからオペランドアドレスを入力し、

該オペランドアドレスを前記メモリにアドレス入力としてのみ供給する、

ように構成されていることを特徴とする処理システム。

【請求項6】 請求項5に記載の処理システムにおいて、

前記オペランドアドレスはオペランドアドレス範囲内に位置し、

前記少なくとも1つのアドレスレジスタの各々は、前記オペランドアドレス範
囲の広がりを含むのに必要とされる最小の大きさとなるように寸法決めされてい
る、

ことを特徴とする処理システム。

【請求項7】 請求項5に記載の処理システムにおいて、

前記プログラム命令のうちの少なくとも1つの命令が、該少なくとも1つの命

令の実行に際して少なくとも2つのアドレスレジスタの修正を実行することを特徴とする処理システム。

【請求項8】 請求項5に記載の処理システムにおいて、

前記プロセッサは、更に、前記オペランドアドレスが零である場合に肯定されるようなアドレス零フラグを供給するように構成され、

前記オペランドアドレスが計数インデックスに対応し、

前記少なくとも1つのアドレスレジスタが、更に、前記プロセッサからのデクリメントコマンドに応答して前記オペランドアドレスをデクリメントし、これにより前記計数インデックスに基づいた計数動作を行うように更に構成されている

ことを特徴とする処理システム。

【請求項9】 請求項5に記載の処理システムにおいて、

前記オペランドアドレスは、下側アドレスと上側アドレスとを有するオペランドアドレス範囲内に位置し、

前記プログラム命令は、

前記少なくとも1つのアドレスレジスタ内のオペランドアドレスをインクリメントすると共に、前記少なくとも1つのアドレスレジスタ内のオペランドアドレスが前記上側アドレスより大きい場合に該少なくとも1つのアドレスレジスタ内の前記オペランドアドレスを前記下側アドレスに一致するようにリセットする巡回インクリメント命令、及び

前記少なくとも1つのアドレスレジスタ内のオペランドアドレスをデクリメントすると共に、前記少なくとも1つのアドレスレジスタ内のオペランドアドレスが前記下側アドレスより小さい場合に該少なくとも1つのアドレスレジスタ内の前記オペランドアドレスを前記上側アドレスに一致するようにリセットする巡回デクリメント命令、

の少なくとも一方を含み、

これにより、前記少なくとも1つのアドレスレジスタにおける前記オペランドアドレスを前記オペランドアドレス範囲内に入るように制限することを特徴とする処理システム。

【請求項10】 請求項9に記載の処理システムにおいて、
前記オペランドアドレスが前記下側アドレスに等しい、及び
前記オペランドアドレスが前記上側アドレスに等しい、
の少なくとも一方に関連する少なくとも1つの条件フラグを更に含むことを特徴とする処理システム。

【請求項11】 プログラム命令を実行するように構成されたプロセッサと

オペランドを含むように構成されたメモリであって、各オペランドが当該メモリ内に対応するオペランドアドレスを有するようなメモリと、
を有する処理システムであって、
前記プロセッサは算術演算ユニットを含み、
前記算術演算ユニットは、
前記メモリに対して、該算術演算ユニットが該メモリのみから第1オペランドを入力するように動作的に結合され、
更に、当該算術演算ユニットの出力及び定数の一方のみから第2オペランドを入力するように構成され、
更に、前記第1オペランド及び第2オペランドの少なくとも一方に基づいて前記出力を生成するように構成されている、
ことを特徴とする処理システム。

【請求項12】 請求項11に記載の処理システムにおいて、
前記算術演算ユニットは、
第1入力と第2入力とを有し、これら第1入力及び第2入力の算術和に対応する前記算術演算ユニットの出力を供給する加算器と、
前記第1入力を、前記第1オペランド及び零値の一方として形成するよう構成された第1オペランドセクタと、
前記第2入力を、前記第2オペランド、該第2オペランドの反転、該第2オペランドのシフト及び零値の内の1つとして形成するよう構成された第2オペランドセクタと、
のみを含むことを特徴とする処理システム。

【請求項13】 プログラム命令を実行するように構成されたプロセッサを有する処理システムであって、

前記プログラム命令の各命令は、複数のフォーマット形式のフォーマット形式に従ってフォーマットされており、

前記複数のフォーマット形式の各フォーマット形式は、各々が各プログラム命令の実行と並列に実行されるべき処理を容易化するような複数のフィールドを有していることを特徴とする処理システム。

【請求項14】 請求項13に記載の処理システムにおいて、

少なくとも1つのフォーマット形式における前記複数のフィールドの略大多数が、少なくとも1つの他のフォーマット形式における前記複数のフィールドの対応する大多数と共通であることを特徴とする処理システム。

【請求項15】 請求項13に記載の処理システムにおいて、

各フォーマット形式における前記複数のフィールドの略大多数が、前記プロセッサ内のスイッチ及び状態装置の動作を制御するマイクロ命令の制御要素に対応していることを特徴とする処理システム。

【請求項16】 請求項13に記載の処理システムにおいて、前記プロセッサは、

各命令を各命令に対応するマイクロ命令に基づいて実行する状態マシンと、

各命令の各制御フィールドを、当該命令のフォーマット形式に応じて、前記マイクロ命令における関連する制御要素に関連付けるフォーマットマップと、

各命令に関連付けられていない前記マイクロ命令の他の制御要素に、デフォルト条件を供給するデフォルト解釈モジュールと、
を有していることを特徴とする処理システム。

【請求項17】 請求項16に記載の処理システムにおいて、前記デフォルト条件が、

前記命令のフォーマット形式、及び

前記命令の少なくとも1つの制御フィールド、

のうちの少なくとも一方にも依存することを特徴とする処理システム。

【請求項18】 請求項16に記載の処理システムにおいて、前記デフォルト

ト条件が、

少なくとも1つの他の制御要素を零値に設定するよう構成されたロード零条件

、
少なくとも1つの他の制御要素に影響されないままで残すよう構成されたヌル条件、

少なくとも1つの他の制御要素を当該命令に含まれる値に設定するよう構成されたロードビット条件、及び

少なくとも1つの他の制御要素に関連する値をインクリメントするように構成されたインクリメント条件、

のうちの少なくとも1つを含むことを特徴とする処理システム。

【請求項19】 請求項13に記載の処理システムにおいて、該システムが

外部データ入力ポート及び外部データ出力ポートを有するメモリであって、これらポートが当該メモリへの及び当該メモリからのデータ項目の記憶及び取り出しを容易化するように構成されたメモリ、

を更に有し、

前記複数のフィールドのうちの少なくとも1つのフィールドは、アドレス選択フィールドを含み、

前記アドレス選択フィールドは外部アドレスポートの選択を容易にし、該外部アドレスポートは、前記外部データ入力ポート及び外部データ出力ポートを介してデータ項目を記憶し及び取り出すために他のプロセッサに前記外部アドレスポートによりアドレス指定される前記メモリのロケーションに対するアクセスを付与するよう構成されている、

ことを特徴とする処理システム。

【請求項20】 請求項13に記載の処理システムにおいて、該処理システムが更に複数の記憶要素を有し、

前記複数のフィールドのうちの少なくとも2つのフィールドは前記複数の記憶要素のうちの少なくとも2つの記憶要素の識別に関連付けられ、

前記プログラム命令のうちの少なくとも1つの命令は、該少なくとも1つの命

令の実行に際して前記少なくとも2つの記憶要素の並列的な変更を容易化する、
ことを特徴とする処理システム。

【発明の詳細な説明】

【0001】

【技術分野】

本発明は処理システムの分野に係り、特に暗号システムに用いるプロセッサに関する。

【0002】

【背景技術】

電子コンテンツ材料を符号化するための暗号の使用は増加しつつある。娯楽分野においては、デジタルオーディオ及びビデオ記録は、当該題材を不正なコピーから保護するために暗号化される。通信分野においては、文書は許可無き看取を防止するために暗号化され、暗号化された証明が文書の認証を検証するために使用される。

【0003】

題材が或る装置から他のものへ伝送される度に、著作権コンテンツ材料、又は斯かる著作権コンテンツ材料へのアクセスに関連するチケットのような安全保護項目を暗号化するための、多数の規格が採用され又は提案されている。例えば、“準拠した”CDレコーダが、複製が保護された題材のコピーを含むCDを作成する場合、該記録は“準拠した”CDプレーヤのみしか該題材を再生することができないように暗号的に保護される。“準拠した”装置とは、採用された規格を実行する装置である。オリジナルの複製が保護されたコンテンツ材料が“1回コピー（copy-once）”なる複製の制限を有している場合、準拠したCDレコーダは、このオリジナルのコピーに“コピー不可（copy-never）”なる表示を暗号的に付す。準拠したCDレコーダは、この“コピー不可”表示を理解して、このコピーのコピーは作成しない。該題材が準拠していないレコーダによりコピーされた場合は、該コピーは適切な暗号項目を含まず、準拠したレコーダ又は再生装置は、このコピーされた題材の記録又は再生を行わない。

【0004】

規格は、Eメール文書及び添付物のような送信されるコンテンツ材料を暗号化し、署名し及び認証するために採用されている。コンテンツ材料が暗号化される

か、及び／又はコンテンツ材料に該コンテンツ材料の送信元を識別するような暗号的な安全保障項目が添付される。該安全保障項目は、該安全保障項目の解読が、該コンテンツ材料が最初に送信されてから変更されたかを識別するような形で該材料に添付又は“結合”される。

【0005】

暗号化及び解読の使用の増加の上記例、及び特に暗号的署名及び検証並びにアクセスチケットの使用の増加は、多様な電子装置への暗号化装置又は解読装置の導入を必要としている。全ての準拠したオーディオ又はビデオ記録又は再生装置は、静止型及び携帯型の装置の両方を含み、キー又は他の安全保障項目を処理し又は交換する手段を含まねばならず、通常は暗号的署名装置若しくは検証装置又は両者を含まなければならない。全てのEメール送信又は受信装置は、携帯電話等の多重機能装置も含め、署名装置若しくは検証装置又は両者を含むことが期待される。このように、多様なシステムにおける暗号的署名、検証及びキーの処理を容易にするような処理装置に対する要望が存在する。

【0006】

特注設計回路は、デジタル署名、検証及び他の認証作業用の暗号化又は解読処理を実施する装置の最も安価な実施例であるかもしれないが、暗号法の発展が、実施化されたアルゴリズムが古くなるという危険性を招来する。汎用のプログラム可能なプロセッサは、実施化されたアルゴリズムを暗号化技術が変化することによって変更することを可能にするが、暗号化能力を要する全ての装置に導入するには必ずしも経済的に可能ではない。低価格汎用プロセッサは、例えばリアルタイムの認証処理に対して期待される目標性能を達成することはできず、補助装置又は高速プロセッサが価格の増加でもって必要とされるであろう。価格の目標が低価格プロセッサ及び補助装置により満たされたとしても、携帯電話等の収容するシステムの物理的制約が、これらの補助装置の使用を排除する可能性がある。

【0007】

【発明の開示】

本発明の1つの目的は、暗号的認証を容易化するプログラム可能な処理システムを提供することにある。また、本発明の他の目的は、共通の暗号化及び解読ユ

一ティリティ機能に対して最適化された暗号処理システムを提供することにある。また、本発明の更に他の目的は低価格な暗号処理システムを提供することにある。

【0008】

これら目的及び他の目的は、暗号処理に特に良好に適したプロセッサアーキテクチャ及び命令セットを提供することにより達成される。設計の複雑さを最小化し、且つ、装置内の相互接続の複雑さを最小化するために種々の技術が使用され、これにより、必要とされる表面面積及び関連する価格を低減する。また、種々の技術が、暗号処理のためにプロセッサをプログラムする作業を容易化し、且つ、スケーラブルな処理のプログラミングで共通に使用されると期待される命令の効率を最適化するために使用される。好ましい低価格の実施例においては、オペランドの記憶用に単一ポートのランダムアクセスメモリ（RAM）が使用され、データ経路には少ないデータバス及びレジスタしか使用されず、命令セットは命令内の並列処理に対して最適化される。暗号処理は幅の広いデータ項目に対する演算を特徴とするので、命令ワードと同じ幅を持つ定数の使用も含め、複数ワード演算の効率的な処理に特に重点を置いた。暗号処理に典型的に必要とされる機能を最小のオーバーヘッドで効率的にサポートする単純化された算術演算ユニットが設けられた。好ましい実施例においては、各命令サイクルにおける複数の並列処理を容易化し、且つ、最小のオーバーヘッドで直接の処理制御を得るように、マイクロコード・マップ型の命令セットが採用された。

【0009】

【発明を実施するための最良の形態】

以下、本発明を例示的に添付図面を参照して詳細に説明する。尚、全図を通して、同一の符号は同様の又は対応する特徴又は機能を示している。また、以下の説明を通して、100と199の間の符号は図1における項目を示し、200と299の間の符号は図2における項目を示し、300と399の間の符号は図3における項目を示し、400と499の間の符号は図4における項目を示す。

【0010】

本発明は、デジタル署名及び検証、公開／私的キーの交換処理等のような暗号

処理は典型的には大きなデータ変数に関わるが、相対的に単純な算術演算処理に関わるものであるという認識に基づいている。認証システム用の通常のアゴリズムは、デジタル署名アルゴリズム(DSA)である。デジタル署名及び検証用の規格(ANSI X9.62)として提案されている他の通常のアゴリズムは、楕円曲線デジタル署名アルゴリズム(ECDSA)である。デジタル伝送コンテンツ保護システム(DTSP)に組み込まれた該アルゴリズムは、IEEE-1394接続を備えるデジタルオーディオ及びビデオ製品に導入されるものとして採用された。上記ECDSAは、低価格実施例に特に良好に適している。何故なら、楕円曲線の使用は、加算、減算、乗算及び反転の単純な数学演算に関わるものであるからである。

【0011】

デジタル署名及び検証に使用されるデータ変数の寸法は大きく、典型的には160又は320ビット幅である。該データ項目を5又は10ワードに均一に分割するために、好ましい実施例においては、32ビット幅のデータワード寸法が使用される。選択されるデータワード寸法は設計上の妥協である。即ち、大きなワード寸法は追加の配線及び経路指定を必要とし、小さなワード寸法はデータ項目当たり追加のワード演算を必要とする。幅広のデータワードには著しい配線及び経路指定のオーバーヘッドが掛かることを認識して、本発明によるデータフロー及び制御構造は従来の処理システムに較べて大幅に制限される。

【0012】

好ましい実施例においては、回路の複雑さ及び経路指定を最小化するために、命令及び定数用の単一のROM、並びに変数用の単一のRAMが好ましい。データ定数は好ましくはデータワードと同一の寸法であり、好ましくは命令と同一のROMに記憶されるので、好ましい実施例における命令ワード寸法はデータワード寸法と等しくする。

【0013】

データ項目に対する上記の単純な数学演算は、必要とされる最小数の命令を示唆し、幅広のデータ項目に適したデータワード寸法に等しい命令ワード寸法は多数の異なる命令を可能にする。処理の速度が重要であることを認識して、各命令に対して利用可能な32ビットは、本発明に従い、各命令内で複数の並列処理を

可能とするように構成される。

【0014】

図1は、本発明による処理システムのデータフローアーキテクチャ100の例示的なブロック図を示している。このブロック図の単純さから判るように、該処理システムは従来の32ビット処理システムと較べて経路指定の複雑さが最小となるように最適化されている。重要なのは、算術演算ユニット(AU)110が単に加算器112と2つの前処理装置114及び116としか有していないことに注意することである。この単純さにより、並列処理を容易化するような演算の一貫性が得られる。更に重要なのは、メモリ120が最小の出力ファンアウトしか備えない単一ポートRAMであることに注意するということである。この最小のファンアウトは、並列処理を容易にする演算の一貫性を提供すると同時に、データ引き回し経路の最小化を可能にする。同様にして、レジスタ130及び140は、AU110の出力111からの単一の入力と、限られた出力とで構成されている。例えば、アドレスレジスタ130の内容は、RAM120をアドレス指定するためにのみ供給され、従来のプロセッサの設計では典型的に普通であったように、AU110又は他の処理装置に対する入力として供給することはできない。レジスタ140は、それ自体では出力を供給せず、以下に述べるように、乗算のような繰り返し演算を制御するための条件ビットを供給するために使用される。このレジスタ130及び140の限られた使用は、各レジスタに必要とされる相互接続の経路指定を最小化し、レジスタ130及び140が、供される機能に対して最適に寸法化されるのを可能にする。例えば、アドレスレジスタ130はメモリ120のアドレス範囲をカバーするのに充分なだけの幅である必要がなく、走査レジスタ140は関連の制御フラグを収容するのに充分なだけの幅である必要しかない。

【0015】

アーキテクチャ100の効率及び有効性が図2に関して最適に図示されており、該図は本発明による2つの例示的な命令フォーマット201及び202を示している。見られるように、命令フォーマット201及び202は、多数の共通な命令フィールドを有している。暗号処理には比較的少ない数の命令形式しか必要

とされないから、各命令につき32ビットを有する命令セットの好ましい実施例は、以下に述べるように、各命令内で並列処理を実行するために各命令内に複数のフィールドの使用を含んでいる。これらの複数のフィールドは、比較的少ない数の命令形式しかサポートしないように構成された従来の幅狭のワード命令セット実施例においては利用可能でないか、又は多数の命令形式をサポートするように構成された幅広のワード命令セット実施例に導入することは不可能であろう。

【0016】

命令フォーマットフィールド210は当該命令に使用された特定のフォーマットを識別し、図示のフォーマット201、202及び他のものの間を区別する。好ましい実施例においては、3ビットが設けられ、これにより8個までの異なるフォーマットをサポートする。本発明によれば、該8個の異なるフォーマットは、命令フィールドのデコードを単純化するために、命令ビットの強い相関を呈している。選択フィールドは異なるフォーマットの各々に対して共通であり、共通に使用される並列処理をフォーマット形式に無関係に実行することができる。例えば、好ましい実施例においては、フィールド230及び240は各フォーマット形式に対して共通であるので、各フィールド230及び240の値により意図される処理、即ちメモリアクセスの制御及び選択は、実行されている特定の命令に無関係に、各命令サイクルの間において実行することができる。フィールド212及び214のような他の共通に使用されるフィールドも、各命令フォーマットに含まれている。また、図4に関して更に後述するように、所与のフォーマット内では利用可能でないフィールドは、比較的に一貫した予測可能な状態でのデフォルト値をとり、これによりフォーマットに無関係に命令間の更なる機能的類似性を与える。

【0017】

“k follows” フィールド212は、後続の“命令”が定数、即ちデータ項目、kを含むことを通知するために使用される。このフィールド212の使用は、少なくとも2つの利点を提供する。即ち、該フィールドは次の命令に含まれる定数kが命令ワード寸法（好ましい実施例においては、32ビット）の全体を占めることを可能にすると共に、該フィールドは次の命令に含まれる該値kが次の命

令サイクルにおいてレジスタ r 0 にロードされるのを可能にする。従来の固定命令寸法の処理システムにおいては、典型的には命令ワード及び定数ワードの両方において、これら2つの間を区別するために1ビットが取って置かれ、これにより定数ワードの寸法を全命令幅より1ビット小さく制限する。図示されていないが、命令内に“定数”フィールドを含むような他のフォーマットが設けられる。これらのフォーマットにおいては、設けられる定数 k は 32 ビットより小さく、k なる 32 ビット定数値に関連する特定されていない上位ビットは、特定のフォーマットに応じて、零で満たされるか又は符号で延長される。これらの k の短縮された値は、典型的には、ベースアドレスに対してメモリアドレスを計算するためのオフセット値として設けられるか、又は現在の命令位置から次に意図する命令に到達するためにどの位遠くへ分岐するかを特定する相対分岐命令用の距離値として設けられる。

【0018】

“更新フラグ” フィールド 214 は、該命令が実行された場合に当該処理システムに関連する条件フラグを修正すべきか否かを識別するために使用される。1999年12月17日に出願された“分離された条件及びアドレスを有する分岐命令”なる名称の同時係属中の米国特許出願第09/466,405号（参照により本明細書に組み込まれる）は、条件フラグが条件命令での後の使用のために何時待避されるべきかの急速識別を含み、分岐命令からの条件評価の分離、及び他の条件命令を開示している。フィールド 214 が肯定的な値を含む場合、キャリー、零及び偶数のような図1の通常のシステムフラグ 118 並びに他の条件フラグは、以下に述べるように、待避され、他の命令がフィールド 214 に肯定的な値を含むまで更新されない。

【0019】

“メモリアクセス制御” フィールド 230 は、メモリ 120 がアクセスされているか、もしそうなら、該メモリが読取動作又は書込動作のためにアクセスされているかを判定する。前述したように、メモリ 120 は単一ポートメモリであって、該メモリ 120 のファンアウトは限られており、これにより比較的単純なメモリアクセス制御を可能にしている。これも前述したように、フィールド 230

は全ての命令に対して共通であり、これにより如何なる他の命令とでも並列にメモリの読み出し及び書き込みを可能にしている。

【0020】

“アドレス選択”フィールド240は、メモリ120をアドレス指定するのにセクタ180の何の入力を使用されるかを決定する。選択されたアドレスは、間接アドレスロケーションIDA185か、AU110の出力111か、外部アドレスextA188か、又はアドレスレジスタ130の1つである。前述したように、全ての命令内にフィールド240を設けたことにより、メモリ選択動作は如何なる他の命令とも並列に実行することができる。従来の処理システムにおいては典型的に見られるような、如何なるレジスタ要素もメモリ120とAU110との間に存在せず、これにより中間の“ロードレジスタ”命令なしで、AU110がメモリ項目に直接アクセスするのを可能にしていることに注意するのも重要である。“被アドレスレジスタ変更”フィールド242は、上記アドレス選択フィールド240と共に動作し、アドレスされたレジスタのインクリメント又はデクリメントを、該インクリメント又はデクリメントされたアドレスにおけるメモリ内容がAU110に供給されるのと同じ命令サイクルの間に可能にする。

1999年12月17日に出願された“巡回アドレスレジスタ”なる名称の同時係属中の米国特許出願第09/466,404号（参照により本明細書に組み込まれる）は、レジスタに対するポインタを自動的に調整して巡回的地址指定機能を提供するような“巡回的インクリメント”及び“巡回的デクリメント”機能を可能にするよう構成された巡回アドレスレジスタを開示している。本発明の好ましい実施例における被アドレスレジスタ変更フィールド242は、アドレス選択フィールド240により決定されたレジスタ130の各々に対する巡回的インクリメント及びデクリメント機能を実行する状態を含む。当業者にとり自明であろうように、全て単一の命令サイクル内で、アドレスを巡回的にインクリメントし、斯様に巡回的にインクリメントされるアドレスの内容をAUに供給し、これら内容に算術演算を実行し、その結果を宛先レジスタ（後述する）に記憶し、及び他のレジスタ（後述する）を巡回的にインクリメントする能力は、複数ワードデータ項目を含む暗号的及び他のアプリケーションに特に良好に適している。

【0021】

外部アドレスextA188が、外部プロセッサが当該処理システム100とは略独立してRAM120にアクセスするのを可能にすることにも注意すべきである。即ち、本発明の好ましい実施例においては、例えば上記アドレス選択フィールドを、RAM120をアドレス指定するためにextA188入力を選択するような適切な値に設定することにより、ホストシステムにRAM120に対するアクセスを付与することができる。この場合、該ホストシステムはextA188によりアドレス指定されたロケーションに対して、extDI入力187を介してRAM120にデータを直接ロードすることができる。この入力データは、例えば、電子文書又はチケットに結合されたハッシュ値、及び該ハッシュ値を暗号化して該文書又はチケットに関連するデジタル署名を形成するために使用されるキーであり得る。斯かるハッシュ値及びキーをロードした後、当該処理システム100は上記RAMに対するアクセスを再び獲得し、適切な暗号化機能を実行して対応するデジタル署名を得るが、該署名はRAM120内に配置されるであろう。次いで、上記ホストシステムにはextA188を介してRAM120へのアクセスが再び付与され、これにより該ホストシステムは上記デジタル署名をRAM120のextA188によりアドレス指定される各ロケーションからデータ出力ポートextDO186を介して読み取る。即ち、本発明の該態様によれば、RAM120に対する外部アドレス指定アクセスを付与することにより、処理システム100はメモリ転送機能を直接サポートする必要はない。

【0022】

次の4つのフィールド、即ち“右オペランド前処理”250、“左オペランド前処理”252、“加算器機能”260及び“nd選択”262は、AU110並びに関連するコンポーネントレジスタr0150及びセレクタ160を制御する。左オペランド前処理フィールド252は、メモリ120のアドレス指定された項目が直接使用されるべきかを決定し、もしそうでないなら、零が左オペランド入力としてAU110に供給される。同様に、nd選択フィールド262は、AU110の出力111か又は定数k165がレジスタr0150に入力として供給されるかを決定する。右オペランド前処理フィールド250は、レ

レジスタr0 150の内容がAU110に対して右オペランドとして供給されるか及びどのように供給されるかを決定する。右オペランド前処理フィールド250は、当該命令の実行の間の並列処理として、レジスタr0 150の内容の加算器112への直接伝達（“無”前処理）、レジスタr0 150の内容の左及び右シフト、又はレジスタr0 150の内容の反転を行う。該フィールドの名称が意味するように、この並列処理は当該命令で特定される算術演算の前に実行される。右オペランド前処理フィールド250は、零値が加算器112の右入力として供給されるのを可能にし、これによりRAM120からの値mdの、RAM120の他のロケーションへの又はレジスタ130、140、150の1つへの転送を容易にする。加算器機能フィールド260は、当該AUへの左及び右入力の加算がキャリー値、又は反転キャリー値、又は定数1の加算を含むかを決定する。このように、前処理機能114及び116並びに加算機能112の組合せは、単項及び2項加算機能、並びに減算及び乗算及び2による除算を可能にする。当業者にとり自明であるように、本発明に従いフィールド250、252及び260により提供されるような、単一命令サイクル内で事前結果をシフトし、これを他のオペランドにキャリービットを伴って加算する能力は、暗号の分野では普通である乗算処理、及び複数ワードデータ項目の乗算を含む他のアプリケーションに特に良好に適している。

【0023】

“宛先レジスタ”フィールド270は、AU110における演算の結果111が何処に経路指定されるかを識別する。前述したように、好ましい実施例における経路指定の複雑さを最小化するために、AU110の出力111のファンアウトは、レジスタ130、140及び該AU110に関連する入力レジスタr0 150に限定されている。

【0024】

“更新レジスタ”フィールド280、及び関連する“更新レジスタ変更”フィールド282は、当該命令の処理の間に実行することが可能な更に他の並列処理を定義する。更新レジスタ変更フィールド282は、巡回的なポインタのインクリメント又はデクリメント処理を含め、更新レジスタフィールド280により識

別される該更新レジスタに対するインクリメント又はデクリメントを実行することができる点で、前記被アドレスレジスタ変更242に類似している。

【0025】

上述したように、命令フォーマット201は、このフォーマットを例えば算術演算等の主機能を実行するために使用する単一命令の実行の間における複数の処理の並列な実行を容易化する。命令フォーマットフィールド210により識別される他の命令フォーマットは、他の主機能を果たし、その際に並列処理も容易化する。

【0026】

図2の命令フォーマット202は、好ましい実施例において他の補助処理と並列な分岐処理又はコール処理のために使用される例示的フォーマットを示している。前述したように、フィールド212、214、230及び240は好ましい実施例においては全ての命令に対して共通であり、また、図2に示すように、フィールド250、252、260及び262はフォーマット201及び202の間で共通である。このように、フィールド212、214、230、240、250、252、260及び262に関連する前述した処理が、分岐又はコール処理が実行されるのと同時に実行される。当業者にとり自明であろうように、当該オペランドを処理するであろう他のルーチンへの分岐又はコールの準備として、オペランドに対してアドレス指定し、ロードし及び算術演算を実行する能力は、暗号法及び他のアプリケーションに通常使用されるような反復処理のための高度に有効且つ効率的な技術を提供する。

【0027】

“条件”フィールド220及び関連する“反転条件”フィールド222は、後続する2つのロケーションのうちのどちらが、実行されるべき次の命令を得るのに使用されるかを決定するために使用される。即ち、条件220が第1状態である場合は、当該プログラムは第1アドレスから進み、それ以外の場合、該プログラムは第2アドレスから進む。反転条件フィールド222は、上述した第1状態が“真”又は“偽”状態のいずれに対応するかを決定する。図2に示したように、好ましい実施例における条件フィールド220は6ビットを使用し、これによ

り64までの異なる条件を判定することができる。特に注意すべきは、フィールド220の条件の1つが、本発明によれば、データ項目=0条件を含み、他の条件がデータ項目=1条件に対応するということである。データ項目=0条件は、複数ワードデータ項目に対応するデータワードの各々が零に等しい場合に真に設定され、データ項目=1条件は、複数ワードデータ項目に対応するデータワードの各々が最下位データワードを除き零に等しく、該最下位データワードが1なる値を含む場合に真に設定される。他の条件項目は、走査レジスタ140に記憶された各ワードの最下位ビット及び最上位ビットのような該走査レジスタ140内の特定のビットの状態を含み、これにより複数ワードの被乗数の効率的な乗算演算を助ける。他の条件項目はアドレスレジスタ130を選択するために使用されるアドレスポインタの状態を含み、複数ワード処理演算の開始及び終了の識別を容易化する。当業者にとり自明であるように、分岐又はコール命令内に64までの異なる条件を設けたことにより、暗号処理において典型的に実施される、複数ワードオペランドの乗算のような複雑な反復演算を制御及び最適化する有効且つ効率的な手段が提供される。

【0028】

“次の命令”フィールド290は、次の各命令が当該処理システムに供給されるアドレスを制御することによりプログラムの流れを制御する。図3は、本発明による処理システム用の制御経路アーキテクチャの例示的なブロック図を示している。各命令331は、図3にROM330として示されたメモリから当該処理システムに供給される。命令アドレス371の順序が、当該処理システムに供給される個々の命令331の順序を決定する。命令331は、図2を参照して説明したようにフォーマットされている。プログラムカウンタ310は、現在の命令アドレス371を含み、セレクト340、350及び370並びに加算器360は、以下に説明するように次の命令フィールド290の状態に基づいて次の命令のアドレスを決定する。

【0029】

本発明の好ましい実施例においては、次の命令フィールド290は次の命令に関する以下の決定を行う：

- i) $pc \leq pc + 1.$ (sequence)
- ii) If (cond) Then $pc \leq k$ Else $pc \leq pc + 1.$ (branch to k if)
- iii) If (cond) Then $pc \leq r0$ Else $pc \leq pc + 1.$ (branch to r0 if)
- iv) If (cond) Then $pc \leq k$; push($pc+1$) Else $pc \leq pc + 1.$ (call if)
- v) If (cond) Then $pc \leq pop$ Else $pc \leq pc + 1.$ (return if)
- vi) If (cond) Then $pc \leq pc + k$ Else $pc \leq pc + 1.$ (r. branch if)
- vii) If (cond) Then $pc \leq k$ Else $pc \leq pop.$ (branch if else return)
- viii) If (cond) Then $pc \leq pc + k$ Else $pc \leq pop.$ (r. branch if else return)

【0030】

当業者にとり自明であるように、最初の次の命令の決定i)は、次の命令への順次の進みであり、プログラムカウンタ pc は1だけ進む。2番目及び3番目の決定ii)及びiii)は、各々、通常の条件分岐である。条件が真の場合（又は、条件が偽であり且つ“反転条件”フィールド222が肯定的である場合）、プログラムカウンタ pc は特定のアドレス k に又は決められたアドレス $r0$ （図1のレジスタ $r0$ 150に含まれる）に設定され、それ以外の場合はプログラムカウンタは1だけ進められる。4番目の決定iv)は、通常の条件コールであり、条件が真の場合は次の順番のアドレス、 $pc + 1$ 、がスタック320にプッシュされ、プログラムカウンタは特定のアドレス k に設定される。5番目の決定v)は通常の条件リターンであり、条件が真の場合は、先にプッシュされたコールの後の次の順番のアドレスがスタック320からポップされ、プログラムカウンタに投入される。6番目の決定vi)は通常の相対分岐命令であり、次の命令のアドレスを決定するために、定数（正又は負）が現在のプログラムカウンタに加算される。単一の加算器360が、プログラムカウンタのインクリメント動作及び相対分岐アドレスの計算の両方を扱うことに注意されたい。

【0031】

特に重要なのは、2つの決定vii)及びviii)に注意することである。本発明の1つの態様によれば、当該命令セットは“Branch If, Else Return”命令を含み

、この場合、条件が真であると当該プログラムは特定のアドレス又は相対アドレスに分岐するが、条件が偽であると当該プログラムは、スタックからリターンアドレスをポップすることによりサブルーチンコールから戻る。条件ステートメント内の“Else Return”構造は反復処理を実行するサブルーチンにおいて特に有効且つ効率的で、ここでは、次の反復を実行するためのアドレスに分岐するか、又は当該反復が完了した際にリターンするために同一の命令が使用される。後続の次の命令を決定する技術の他の変形例は、当業者にとり本開示から明であろう。

【0032】

図4は、上述した機能及び能力を提供する有効且つ効率的な構成を呈するプロセッサ400の例示的なブロック図を示している。図4の例において、処理回路450はマイクロコード命令455に応答して動作し、該マイクロコード命令は当該処理回路450内の各スイッチ及び状態装置を制御する制御ビット455bを有している。即ち、例えば処理回路450は典型的には状態マシンを有し、上記マイクロコード命令455は該状態マシンに入力刺激を与え、該刺激は次の状態への移行を制御すると共に該状態マシンからの出力の生成を制御する。マイクロコード命令455は、例えば、制御ビットを有し、該制御ビットは、図1のセクタ160が当該マイクロコード命令455に含まれる定数k455aか又は算術演算ユニットAU110の出力結果111かのいずれをレジスタr0150に供給するように設定されるかを決定する。該マイクロコード命令は、更に、RAM120をアドレス指定するためにセクタ180によりどのアドレス入力が選択されるかを決定する一連の制御ビット、前処理装置116により実行される処理を決定する一連の制御ビット、前処理装置114により実行される処理を決定する一連の制御ビット等も含む。命令フォーマット201、202内の前述したフィールドが、これらのマイクロコード制御ビット455bに略対応することが理解されるであろう。即ち、本発明の該態様によれば、マイクロコード命令455の選択要素に略対応するような命令フォーマット201、202のフィールドが設けられ、これにより、基礎となる処理回路450の最小のオーバーヘッドでの直接制御を容易化している。

【0033】

図4に示すように、命令331の制御フィールド410、即ちフォーマットフィールド210以外のフィールドは、フォーマットマップ及びデフォルト装置440に入力として供給され、該装置は命令331の各制御フィールド410をマイクロコード455内の対応する制御要素にマップする。定数k 455aと制御ビット455bの両方が、処理回路450により提供される演算及び結果に影響を与え、マイクロコード455の制御要素の定義に含まれることに注意すべきである。

【0034】

マップ/デフォルト装置440は複数のセクタ441ないし449を有し、これらセクタは、命令311の所与のフォーマット210に応じて、対応する制御ビット455bへの制御フィールド410の各ビットの経路指定を行なう。即ち、例えば図2において、異なる命令フォーマット201及び202は当該命令のビット位置23ないし31に異なるフィールド(242、280、282)及び(290、220)を含んでいる。マップ/デフォルト装置440は、異なるフィールドを、命令の同一のビット位置からマイクロコード命令の異なる制御要素へ命令331のフォーマット210に応じて経路指定する。

【0035】

本発明の他の態様によれば、マップ/デフォルト装置440は、命令331からのマップされたフィールドがない場合は、各制御要素455に対してデフォルト制御値を供給することによりマイクロコード命令455の制御要素を適切に制御する。即ち、例えば例示した命令フォーマット201、202が、マイクロコード命令455にk 455aの値を設定する定数フィールドを含まないとする。好ましい実施例における命令331の特定の定数フィールドがない場合のデフォルトの解釈は、ヌル動作である。即ち、特定の定数値がない場合は、値k 455aは同一のままとなる。他の例として、当該命令が肯定的な“k-follows”フィールド212を含む場合は、ROM330から読み出される次の命令331は、マイクロコード命令455の定数k 455aに完全にマップされる。(理解を容易にするために、型式マップ440は命令331のフォーマットフィールド

ド210のみを制御入力として入力するように図示されている。上記“k-follows”機能をサポートするには、型式マップ/デフォルト装置440は、前の命令が肯定的なk-followsフィールド212を含む場合に命令331全体をマイクロコード命令455の定数k区域455aに経路指定するように構成される。）

【0036】

好ましい実施例においては、各制御要素455に関連するマルチプレクサ/セレクトアの出力はフォーマットフィールド210の内容に依存し、入力は利用可能なデフォルトオプションに依存する。例えば、前述したように、好ましい実施例の1以上のフォーマット形式（図示略）は当該命令ワードの全幅より小さな定数フィールドを有している。これらのフォーマット形式が入力された場合、対応するマルチプレクサ441ないし449は、定数k 445aの特定されていない上位ビット位置の各々に配置する零値又は符号延長された値を選択するように構成される。例えば、当該命令の定数フィールドが6ビットを含む場合、32ビットの定数k 445aの上位の26ビットは、特定のフォーマット形式に応じて、零なるデフォルト値、又は特定されている6ビットの最上位ビットに等しいデフォルト値（符号拡張された値）に設定され得る。制御ビット455bにもデフォルト値が供給され、殆どの場合ヌル動作となる。マイクロコード命令455の各制御要素に対するデフォルトの値又は条件の選択は、如何なる値又は条件でもよいが、好ましい実施例においては、デフォルトの値及び条件は、当業者により推定される値と一貫したものに選定される。即ち、例えば短縮されたデータ定数が供給される場合は上位ビットの零化が、アドレスのオフセットが供給された場合は上位ビットの符号延長が、当業者により適切なデフォルトであるとみなされるであろう。同様に、フォーマット202の次の命令フィールド290に対応する制御ビット群のデフォルト条件は、1命令によるプログラムカウンタの進みに対応すると見なされるであろう。即ち、次の命令フィールド290を含まないフォーマット201を有する命令が入力された場合、デフォルト解釈モジュール440は、存在しないフィールド290に対応するマイクロコード命令455の適切な制御要素を、セレクトア340、350及び370がプログラムカウンタ310のインクリメントを実行するような適切な入力を選択するように設定されるよ

うに設定し、これにより明示的な命令フィールドがない場合に、一貫した、予測可能な且つ論理的な効果を付与する。

【0037】

上記説明は、本発明の原理を単に示すのみである。かくして、当業者であれば、本明細書には明示的に記載又は示されていないが本発明の原理を具現化し、従って本発明の趣旨及び範囲内に入るような種々の構成を実施化することができることが分かるであろう。例えば、データ項目の複数ワードに基づいて決定される条件に関しては、乗算及び加算のような複数ワード演算の制御を容易化するために、データ項目内の最上位の非零ワードを識別する条件要素を定義することができる。図示された設計の複雑さを最小化するための他の技術も可能である。例えば、図1における間接アドレスポインタIDA 185は、RAM120のアドレス0のような所定のアドレスとして、間接アドレスにアクセスするのに要する回路及び時間を最小化することもできる。同様にして、アドレスレジスタ130によりアドレス指定されるデータ項目がメモリ120の特定の領域内に入るように制限して、該レジスタ130が全メモリ120をカバーするに要する幅というよりは、例えばオフセットベースアドレスを使用して上記特定の領域内のアドレスをカバーするのに要する最小の幅のものとすることもできる。また、ここで提示された原理は暗号アプリケーションに特に良好に適しているが、本開示において提示された技術及び構成は、他のアプリケーションに特化された処理システム、特に幅広のデータ項目を使用し及び／又は比較的単純ではあるが反復的な演算を採用しているようなアプリケーションに適用することもできる。同様に、上記例示実施例は、本明細書においては低製造コストを達成するために最小限の形態で示されているが、性能を向上させるため又はプログラミング作業を容易化するために付加的能力を追加することもできる。図に示された例は解説目的で提示されたものである。例えば、図1には、RAM120をアドレス指定するための最小の経路指定及び相互接続領域を提供するような単一ポートRAM120が示されている。2ポートRAM又は3ポートRAMのような複ポートRAM、及び多重アドレス指定能力に適合した関連するフォーマット形式は、上述した原理を採用することにより、同一命令サイクル内での多重メモリアクセス、及びメモ

リアクセス前のメモリアドレスのプリセット等を可能にするであろう。本発明に鑑み、当業者にとっては他のシステム構成、アプリケーション及び最適化技術が自明であろうし、添付請求項の趣旨及び範囲内に入るであろう。

【図面の簡単な説明】

【図1】

図1は、本発明による暗号処理システム用のデータ経路アーキテクチャの例示的ブロック図を示す。

【図2】

図2は、本発明による暗号処理システム用の例示的な1対の命令セットのフォーマットを示す。

【図3】

図3は、本発明による暗号処理システム用の制御経路アーキテクチャの例示的ブロック図を示す。

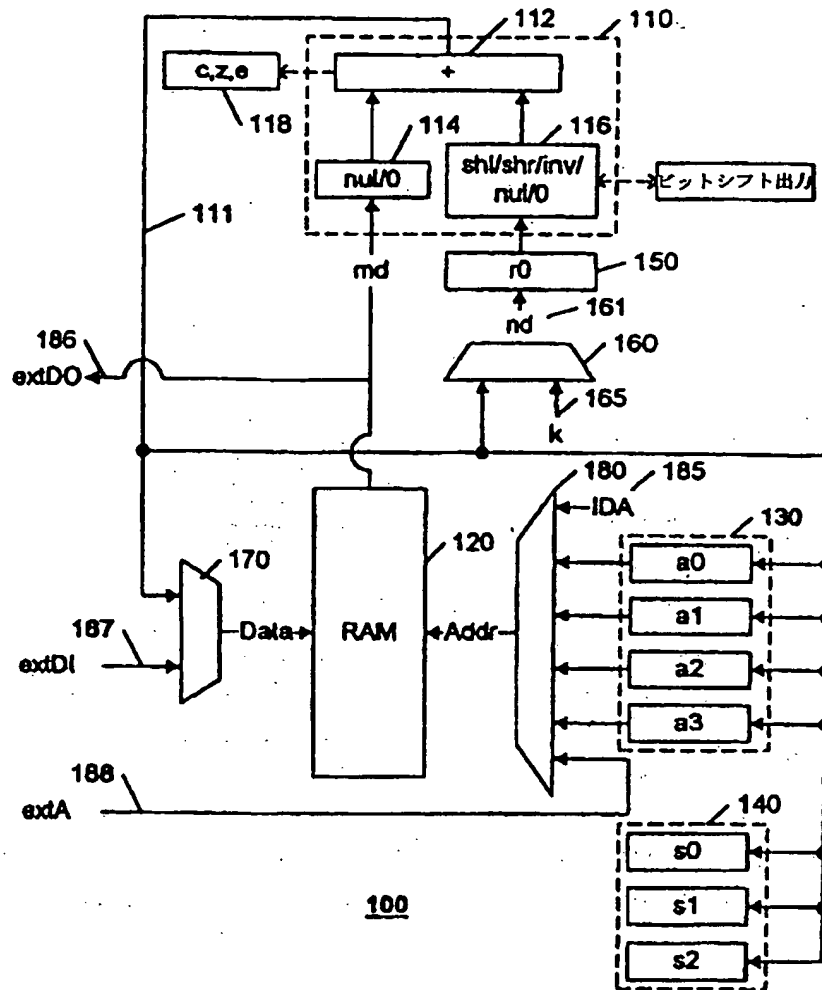
【図4】

図4は、本発明による暗号プロセッサ用のマイクロ命令のマッピングの例示的ブロック図を示す。

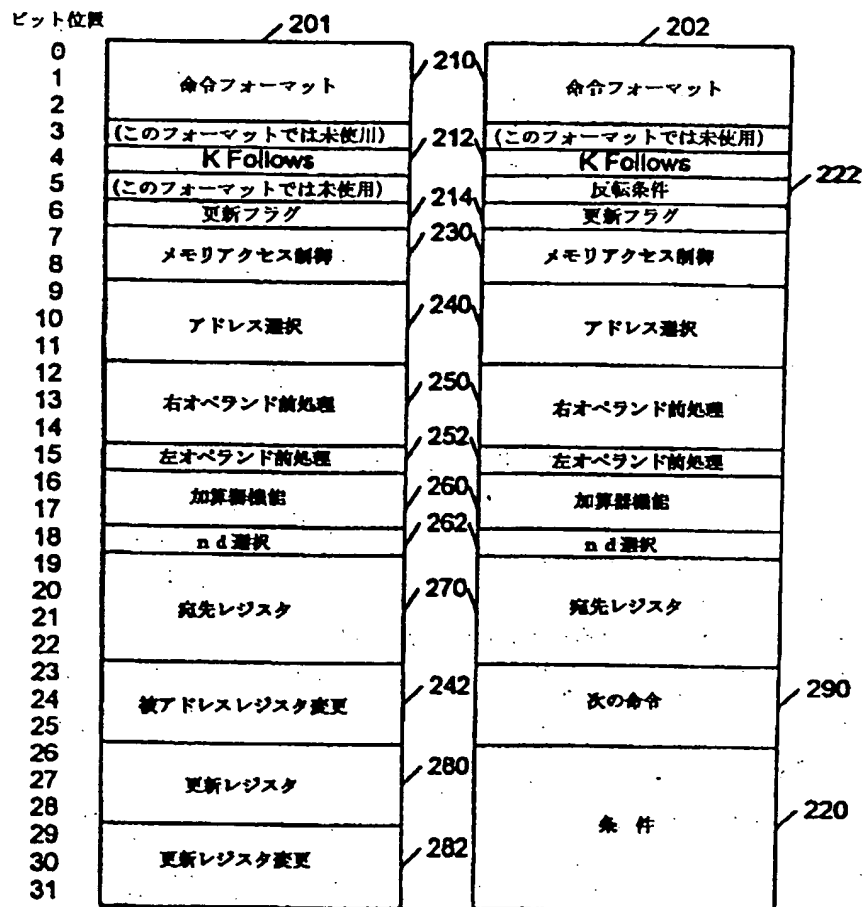
【符号の説明】

- 110…算術演算ユニット (AU)
- 112…加算器
- 114…前処理装置
- 116…前処理装置
- 118…システムフラグ
- 120…メモリ (RAM)
- 130…アドレスレジスタ
- 140…レジスタ
- 150…レジスタ r0
- 160…セレクタ
- 180…セレクタ
- 185…間接アドレスロケーション (IDA)

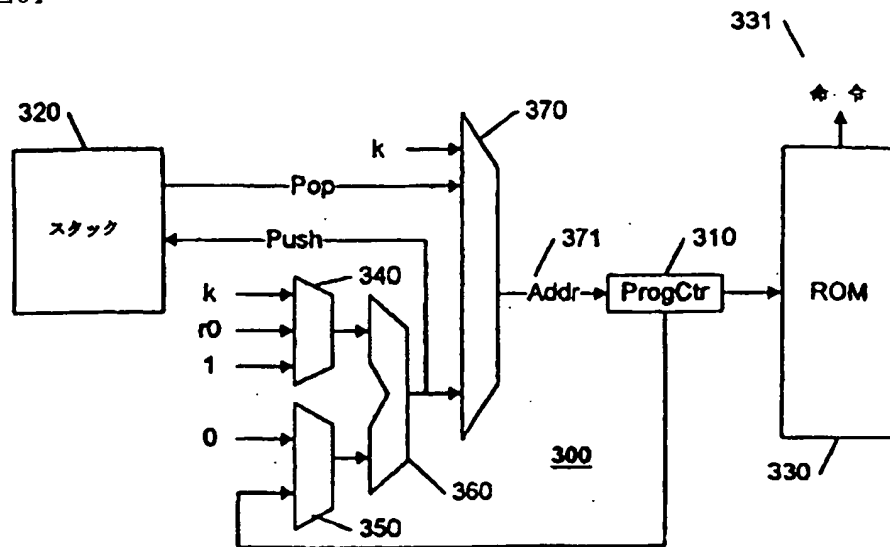
【図1】



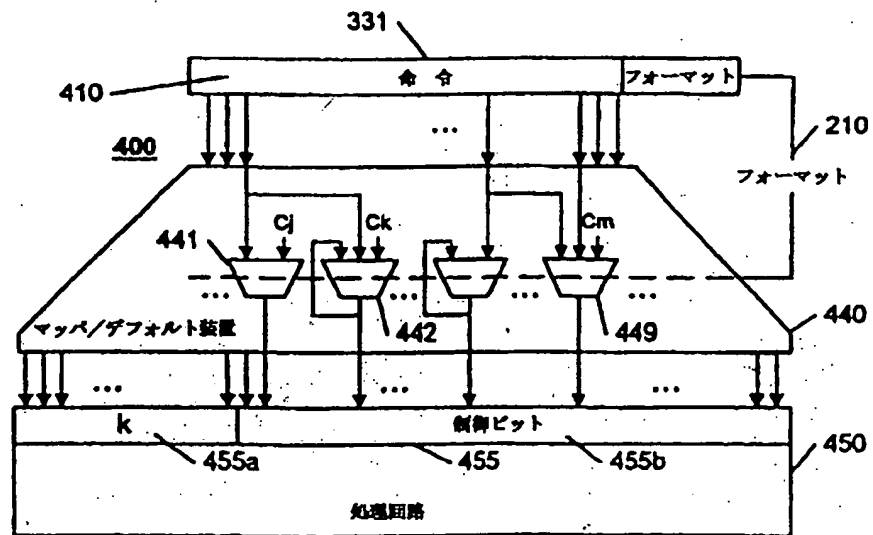
【図2】



【図3】



【図4】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP 00/12441

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 686F9/32		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 686F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EP0-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 161 247 A (WAKABAYASHI TAKAO ET AL) 3 November 1992 (1992-11-03) column 14, line 64 -column 15, line 27 ---	1
A	WO 99 26135 A (ADVANCED MICRO DEVICES INC) 27 May 1999 (1999-05-27) page 15, line 33 -page 16, line 7 ---	1
A	US 5 539 888 A (BYERS LARRY L ET AL) 23 July 1996 (1996-07-23) column 11, line 28 -column 12, line 21 -----	1
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another document or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the actual completion of the international search 22 August 2001		Date of making of the international search report 22 Jan 2002
Name and mailing address of the ISA European Patent Office, P.O. 5618 Patanden 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Te. 31 851 epo nl, Fax: (+31-70) 340-3016		Authorized officer Moraiti, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP 00/12441

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/EP 00/12441

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claim : 1

Branch-else-return instruction

2. Claims: 2-10

Multigauge processor with status register

3. Claims: 11,12

Arithmetic Unit

4. Claims: 13-20

Formatted program instructions

INTERNATIONAL SEARCH REPORT
 information on patent family members

 International Application No.
PCT/EP 00/12441

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5161247 A	03-11-1992	JP 1958306 C	10-08-1995
		JP 2162914 A	22-06-1990
		JP 6083019 B	19-10-1994
		JP 2163862 A	25-06-1990
		JP 2577071 B	29-01-1997
		JP 2181870 A	16-07-1990
		JP 2187824 A	24-07-1990
		JP 2187829 A	24-07-1990
		JP 2189087 A	25-07-1990
		CA 1311063 A	01-12-1992
		DE 68927798 D	03-04-1997
		EP 8373291 A	20-06-1990
		EP 8666532 A	09-08-1995
		EP 8669599 A	30-08-1995
		EP 8666533 A	09-08-1995
		KR 9210933 B	24-12-1992
		US 5421823 A	30-05-1995
		US 5504916 A	02-04-1996
		US 5388236 A	07-02-1995
		US 5442799 A	15-08-1995
WO 9926135 A	27-05-1999	US 6167506 A	26-12-2000
		DE 69802562 D	20-12-2001
		EP 1031075 A	30-08-2000
		EP 1031074 A	30-08-2000
		JP 2001523854 T	27-11-2001
		US 6134649 A	17-10-2000
		WO 9926132 A	27-05-1999
		US 6199154 B	06-03-2001
		US 6256728 B	03-07-2001
		US 6112293 A	29-08-2000
		US 6219784 B	17-04-2001
		US 6067786 A	30-05-2000
US 5539888 A	23-07-1996	NONE	

フロントページの続き

(72)発明者 オストラー ファーレル エル
オランダ国 5656 アーアー アイन्दー
フェン プロフ ホルストラーン 6

(72)発明者 ダゲール アントニー エフ
オランダ国 5656 アーアー アイन्दー
フェン プロフ ホルストラーン 6

Fターム(参考) 5B013 DD00 DD06

5B033 AA01 AA03 AA09 AA14 AA17

BA01 BD02 BD04 BE00 DE07

5J104 AA18 NA39

【要約の続き】

するため、及び最小のオーバーヘッドで直接的処理制御
を行うために、好ましい実施例においてはマイクロコー
ド-マップ型の命令セットが使用される。